Title: AFFIDAVIT OF DIGITAL EVIDENCE — CHAIN OF CUSTODY AND SYSTEMIC INTRUSION REPORT

Prepared By: John Fouts
Date: May 25, 2025
Document Source: temp-test-OCR-reprocess.pdf (230-page OCR-processed forensic log)

I. DECLARATION

I, John Fouts, do solemnly declare and affirm under penalty of perjury that the contents of this document are true and accurate to the best of my knowledge and belief. This report comprises direct forensic evidence extracted from my personal digital systems, which have been compromised through unauthorized access, persistent surveillance, and network interference, in violation of federal communications, civil rights, and privacy law.

II. PURPOSE OF DOCUMENT

This affidavit provides:

1. A summary of key findings from forensic log records.
2. A detailed incident timeline extracted from verified file metadata.
3. Evidence to support immediate regulatory and legal action.
4. A demand that T-Mobile, and relevant network partners, be required to:
    - Disclose full tower connection logs and routing history.
    - Refer the matter to CISA, IC3, and appropriate federal authorities.
    - Cooperate with criminal and civil investigations into retaliation and color of law violations.

III. EVIDENCE SUMMARY

A. Forensic Signatures of Compromise:

- Persistent access to directories such as `C:\Users\John\AppData\Local\TelemetryCache`, `ConnectedDevicesPlatform`, `ETL logs`, and `SystemData`.
- Unusual sequences in file timestamps (e.g., files accessed before creation).
- Recurrent triggering of diagnostic and logging files (e.g., `Microsoft-Windows-DxgKrnl.ETL`), which are typically enabled in device monitoring or screen recording scenarios.
- System-wide thumbcache and metadata generation consistent with remote viewing of files.

B. Visual Analysis Evidence:

- Screenshots and captures embedded in the 230-page PDF document display manipulated or spoofed IP/MAC configurations, unauthorized device pairing, and mirror-image UI inconsistencies suggesting OS virtualization or cloaked VMs.
- Device logs include attempts at BIOS/UEFI-level hooks, referencing paths such as `\Recovery\OEM\` and `Intel\Wireless` tools.

C. Institutional Failures:

- Despite confirmed forensic evidence, T-Mobile repeatedly denied escalation to network security or legal departments.
- T-Mobile refused to provide routing, tower, and session logs upon multiple requests.
- All attempts to report to local law enforcement were refused on grounds of jurisdiction, with the officers stating that the complaint must be initiated by a federal agency.

IV. INCIDENT TIMELINE (SELECT ENTRIES)

Timestamp	Event Description
2023-08-02 01:13:04	Modification of `John\Favorites\Links` - potential injection of tracking or spoofed content.
2023-08-02 01:13:05	ETL trace logs accessed and generated.
2023-08-02 01:13:08	Multiple telemetry and diagnostic cache files created/accessed.
2023-08-02 01:13:14	Unauthorized access to shared directories like `Public\Documents\Wondershare`.
2023-08-02 01:13:23	Final cluster of access shows orchestration of file system activity across multiple accounts.

V. DEMAND FOR CORRECTIVE ACTION

Given the systemic nature of this intrusion and T-Mobile's documented refusal to investigate or notify authorities:

- I hereby demand that the FCC, FTC, CISA, and IC3 mandate that T-Mobile release all connection, routing, and diagnostic logs for my account, and that FCC, FTC, CISA, and IC3 review the entirety of the data available via forensic expert analysis to show what I have already proven from another source. At this time other independent reviewers are also analyzing the data to ensure accountability and integrity from government agencies.
- T-Mobile must be required to provide formal documentation to federal law enforcement. I demand T-Mobile pursue a formal legal law enforcement official report, rather than placing the

investigatory burden solely on the consumer, who does not control or manage the compromised infrastructure, aside from the end-user device and retail service access.

- I demand a third-party neutral cybersecurity firm audit the data and network behavior retroactive to early 2023.

VI. SUPPORTING FILES AND MATERIALS

This affidavit is accompanied by:

- Original forensic document: `temp-test-OCR-reprocess.pdf`
- Annotated screenshots of Gmail security alerts indicating account hijack and spoofed authentications.
- Cellular tower field data and screenshots indicating rogue or non-attributable tower connections.
- Screenshots of system-level logs and behavior during known intrusion windows.

VII. SIGNATURE & VERIFICATION

I, John R. Fouts, affirm that the above is true to the best of my ability and understanding, and that the original logs were generated directly from my hardware without any tampering or artificial manipulation.

Signed,
John Fouts
Louisville, KY
Date: May 25, 2025

Appendix A

- See `2025-05-25-TMobile_Visual_Evidence_annotated_Shows-Connection_To_Rogue_Towers_And_Other_Confirmed_Compromise_FCC-J.pdf` for full visual and forensic support.